UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/655,229	09/05/2000	Chung Nan Chang	2174	7777

7590 12/29/2005

Donald E Schreiber
Donald E Schreiber A Professional Corp.
Post Office Box 2926
Kings Beach, CA 96143-2926

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/655,229	CHANG, CHUNG NAN	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 have been examined.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-29 are provisionally rejected on the ground of nonstatutory double patenting over claims 1-41 of copending Application No. 09/655,230. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows: both receiving and transmitting unit store and retrieve plurality of public quantities to compute key in order to transmit cyphertext message over insecure channel.

Furthermore, there is no apparent reason why applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Crandall U.S. Pat. No. 5805703 (hereinafter Crandall).

6. As per claim 1, Crandall discloses a protocol for cryptographic communication via a communication channel "I" in which a sending cryptographic unit "S" transmits onto the communication channel I an encrypted ciphertext message "M" obtained by supplying both a plaintext message "P" and a cryptographic key "K" to a first cryptographic device, and in which a receiving cryptographic unit "R" receives the ciphertext message M from the communication channel I and by supplying the ciphertext message M together with the key K to a second cryptographic device decrypts the plaintext message P therefrom (Crandall: summary: conventional cryptographic communication), a method by which the units S and R mutually

establish a cryptographic key K by first exchanging messages before the sending unit S transmits the ciphertext message M comprising the steps of:

the sending unit S:

retrieving the plurality of public quantities from the publicly accessible repository (Crandall: column 13 lines 18-30 and figure 12: the sender uses public storage information to generate key);

using at least some of the plurality of public quantities, computing and transmitting to the receiving unit R a plurality of sender's quantities (Crandall: column 19: lines 42-48: plurality of sender's quantities are ciphertext message and signature); and

using at least one of the plurality of public quantities, computing the key K (Crandall: column 13 lines 18-30); and c. the receiving unit R, using at least one of the plurality of sender's quantities received from the sending unit S computing the key K (Crandall: figure 12 and column 20 lines 42-52: the using sender's public key to compute deciphering key).

Crandall does not explicitly disclose the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines 15-24 and figure 12: store publicly known information). It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit.

7. As per claim 2, Crandall further discloses the method of claim 1 wherein the receiving unit R, in storing the plurality of public quantities into the publicly accessible repository (Crandall: column 20 lines 15-24: stores publicly known information):

selects at least one receiver's secret quantity (Crandall: column 8 lines 16-20 and figure 3: receiver's public key is produced by using its private key);

selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity (Crandall: column 15 lines 28-33); and

using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities (Crandall: column 15 lines 34-38 and column 8 lines 16-20).

8. As per claim 3-5, Crandall further discloses the method of claim 2 wherein the plurality of public quantities/computed public quantities/selected public quantity include a plurality of vectors (Crandall: column 20 lines 15-24: sender's and receiver's public keys and curve parameter.., etc. ; column 8 lines 8-42: how public keys are generated).

9. As per claim 6, Crandall further discloses the method of claim 2 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R (Crandall: column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver):

selects a sender's secret quantity (Crandall: column 13 lines 18-30: take the sender's private key); and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities

(Crandall: column 13 lines 18-30: generate enciphering key to encipher the plaintext; column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver as plurality of quantities).

10. As per claim 7, Crandall further discloses the method of claim 6 wherein the plurality of sender's quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature (u,P) is sent to the receiver; column 16 – column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

11. As per claim 8, Crandall further discloses the method of claim 1 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving unit R (Crandall: column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver):

12. selects a sender's secret quantity (Crandall: column 13 lines 18-30: take the sender's private key); and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit "R" the plurality of sender's quantities (Crandall: column 13 lines 18-30: generate enciphering key to encipher the plaintext; column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver as plurality of quantities).

13. As per claim 9, Crandall further discloses the method of claim 8 wherein the plurality of sender's quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature (u,P) is sent to the receiver; column 16 – column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

14. As per claim 10 and 19, Crandall discloses a system adapted for communicating as an encrypted ciphertext message M a plaintext message P that has been encoded using a cryptographic key K, the system comprising:

a communication channel I adapted for transmitting the ciphertext message M (Crandall: summary: conventional cryptographic communication);

a pair of transceivers that are coupled to said communication channel I, and that are adapted for communicating the ciphertext message M from one transceiver to the other transceiver via said communication channel I (Crandall: summary: conventional cryptographic communication); and

a pair of cryptographic: units each of which is respectively coupled to one of said transceivers for transmitting the ciphertext message M thereto or receiving the ciphertext message M therefrom (Crandall: summary: conventional cryptographic communication), each cryptographic unit:

when the cryptographic unit is to receive the ciphertext message M:

receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit (Crandall: column 19: lines 42-48 and figure 12: plurality of sender's quantities are ciphertext message and signature), and using at least one of the plurality of sender's quantities in computing the key K (Crandall: column 13 lines 18-30); and

when the cryptographic unit is to send the ciphertext message M, retrieving the plurality of public quantities from the publicly accessible repository (Crandall: column 13 lines 18-30 and figure 12: the sender uses public storage information to generate key) and using:

at least some of the plurality of public quantities in computing the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit (Crandall: column 19: lines 42-48: plurality of sender's quantities are ciphertext message and signature); and

at least one of the plurality of public quantities in computing the key K (Crandall: column 13 lines 18-30) ; and

including a cryptographic device having:

a key input port for receiving the key K from the cryptographic unit (Crandall: figure 12 and column 20 lines 25-41: the cryptography device is provided the key);

a plaintext port (Crandall: figure 12 and column 20 lines 25-41: the cryptography device is provided key along with plaintext):

for accepting the plaintext message P for encryption into the ciphertext message M that is transmitted from the cryptographic device (Crandall: figure 12 and column 20 lines 25-41: generate ciphertext and send it); and

for delivering the plaintext message P obtained by decrypting the ciphertext message M received by the cryptographic device (Crandall: column 20 lines 42-52 and figure 12); and

a ciphertext port that is coupled to one of said transceivers:

for transmitting the ciphertext message M to such transceiver (Crandall: figure 12: the cryptography device sends the ciphertext), and

for receiving the ciphertext message M from such transceiver (Crandall: figure 12: the cryptography device receives the ciphertext).

Crandall does not explicitly disclose the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines 15-24 and figure 12: store publicly known information). It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit.

15. As per claim 11 and 20, Crandall further discloses the system of claims 10 and 19 wherein said cryptographic unit which receives the ciphertext message M in storing the plurality of public quantities into the publicly accessible repository (Crandall: column 20 lines 15-24: stores publicly known information):

selects at least one receiver's secret quantity (Crandall: column 8 lines 16-20 and figure 3: receiver's public key is produced by using its private key);

selects for storage in the publicly accessible repository as part of the plurality of public quantities at least one selected public quantity (Crandall: column 15 lines 28-33); and

using the receiver's secret quantity and the at least one selected public quantity, computes and stores in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities (Crandall: column 15 lines 34-38 and column 8 lines 16-20).

16. As per claim 12-14 and 21-23, Crandall further discloses the system of claims 11 and 19 wherein the plurality of public quantities/computed public quantities/selected public quantity

include a plurality of vectors (Crandall: column 20 lines 15-24: sender's and receiver's public keys and curve parameter.., etc. ; column 8 lines 8-42: how public keys are generated).

17. As per claim 15 and 24, Crandall further discloses the system of claims 11 and 19 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit (Crandall: column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver):

selects a sender's secret quantity (Crandall: column 13 lines 18-30: take the sender's private key); and

using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving unit R the plurality of sender's quantities (Crandall: column 13 lines 18-30: generate enciphering key to encipher the plaintext; column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver as plurality of quantities).

18. As per claim 16 and 25, Crandall further discloses the system of claims 15 and 24 wherein the plurality of sender's quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature (u,P) is sent to the receiver; column 16 – column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

19. As per claim 17 and 26, Crandall further discloses the system of claims 10 and 19 wherein the sending unit S, in computing the plurality of sender's quantities for transmission to the receiving cryptographic unit (Crandall: column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver):

selects a sender's secret quantity (Crandall: column 13 lines 18-30: take the sender's private key); and

ii. using the sender's secret quantity and at least some of the retrieved plurality of public quantities, computes for transmission to the receiving cryptographic unit the plurality of sender's quantities (Crandall: column 13 lines 18-30: generate enciphering key to encipher the plaintext; column 19 lines 42-48 and figure 12: ciphertext and signature are sent to the receiver as plurality of quantities).

20. As per claim 18 and 27, Crandall further discloses the system of claims 17 and 16 wherein the plurality of sender's quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature (u,P) is sent to the receiver; column 16 – column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

21. As per claim 28, Crandall discloses a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature (Crandall: summary: communication channel; column 19 lines 42-48: send ciphertext and digital signature), and, wherein before transmitting the message M and the digital signature, a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature (Crandall: column 16 lines 63-67: authenticate the digital signature) comprising the steps performed by the receiving unit R of:

retrieving the plurality of public quantities from the publicly accessible repository (Crandall: column 17 lines 1-50);

using the digital signature and the plurality of public quantities, evaluating expressions of at least two (2) different verification relationships (Crandall: column 17 lines 44-50: two different equations); and

comparing pairs, of results obtained by evaluating the expressions of the at least two (2) different verification relationships (Crandall: column 17 lines 49-50: the digital signature is assumed authenticated when Q and R match).

Crandall does not explicitly disclose the transmitting unit S transmitting for storage in a publicly accessible repository a plurality of public quantities. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines 15-24 and figure 12: store publicly known information). It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit.

22. As per claim 29, Crandall further discloses the method of claim 28 wherein the plurality of public quantities include a plurality of vectors (Crandall: column 19 lines 42-48: the signature (u,P) is sent to the receiver; column 16 – column 17: two points on the curve; column 8 lines 35-36: form an abelian group).

Response to Arguments

23. Applicant's arguments with respect to claims 1-29 have been considered but are moot in view of the new ground(s) of rejection.

24. The application has been re-opened for prosecution in response to Appeal Brief filed on 10/6/05.

Conclusion

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Chang et al. U.S. Pat. No. 5835592 discloses secure, swift cryptographic key exchange.

Bellare et al. U.S. Pat. No. 5491750 discloses method for three-party entity authentication and key distribution using message authentication codes.

Immonen U.S. Pat. No. 6931528 discloses secure handshake protocol.

Boneh et al. U.S. Pat. No. 6965673 discloses method of using transient faults to verify the security of a cryptosystem.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100